MARK R. WARNER
VIRGINIA

886

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

October 25, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

Dear Chairman Wheeler,

I have watched with growing concern over the past two months as an ever-larger network of infected devices has been leveraged to conduct the largest series of Distributed Denial of Service (DDoS) attacks ever recorded. According to global telecommunications provider Level 3 Communications, the 'Mirai botnet' has more than doubled since the source code was first made public on October 1st.[1] The Mirai botnet functions by taking control of highly insecure devices, such as 'Internet of Things' (IoT) products, and using them to send debilitating levels of network traffic from these compromised devices to particular sites, web-hosting servers, and internet infrastructure providers.[2] By infecting consumer devices with this malware, attackers can hijack the communications capabilities of users' devices, using large numbers of them to flood sites and servers with overwhelming traffic. As the co-Chair of the Senate Cybersecurity Caucus, I invite your prompt response to a number of important questions raised by these incidents.

While the precise form of Mirai's attacks is not new, the scale of these volumetric attacks is unprecedented. The weak security of many IoT devices provides an attractive target for DDoS attackers, leveraging the bandwidth and processing resources of millions of connected devices. Botnets are frequently referred to as "zombie computers" and the metaphor is fitting: bad actors infect unsuspecting computers and network devices with malware, sending remote commands to hordes of compromised computers. Analysts have also noted the dynamic nature of Mirai Command and Control (C&C) servers (platforms used by attackers to send these remote commands to the botnets), with the malicious operator or operators switching C&C servers far more rapidly than in past botnet attacks. The United States Computer Emergency Readiness Team (US-CERT) notes in its alert that the release of the Mirai source code has increased the risk of similar botnets being created, acknowledging at least one new separate malware family leveraging IoT vulnerabilities in a manner similar to Mirai.[3]

Mirai's efficacy depends, in large part, on the unacceptably low level of security inherent in a vast array of network devices. Attackers perform wide-ranging scans of IP addresses, searching

[1] Level 3 Threat Research Labs, *How the Grinch Stole IoT* (October 18, 2016), http://blog.level3.com/security/grinch-stole-iot/.
[2] *See* Brian Krebs, *DDoS on Dyn Impacts Twitter, Spotify, Reddit,* KrebsOnSecurity (October 16, 2016), https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.
[3] US-CERT, *Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets* (October 14, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A.

for devices with poor security features such as factory default or hard-coded (*i.e.,* unchangeable) passwords, publicly accessible remote administration ports (akin to open doors), and susceptibility to brute force attacks.[4] In my June 6th letter to the Federal Trade Commission (FTC), I raised serious concerns with the proliferation of these insecure connected consumer products, noting that the "ever-declining cost of digital storage and internet connectivity have made it possible to connect an unimaginable range of products and services to the Internet," potentially without adequate market incentives to adopt appropriate privacy and security measures. Juniper Research has projected that by the end of 2020, the number of IoT devices will grow from 13.4 to 38.5 billion – yet there is no requirement that devices incorporate even minimal levels of security. The internet's open architecture has been a catalyst for its growth, allowing an enormous range of devices and services to connect to a global, interoperable network. The lack of gating functions, however, has potentially created a systemic risk to the resiliency of the internet.

Additionally, the global nature of the supply chain for such devices requires attention not just to the final product integrator's practices, but also to that of suppliers throughout the manufacturing process. In the recent Mirai botnet, researchers have identified a single software supplier as responsible for vulnerabilities in a wide range of manufacturers' products, with Flashpoint concluding that over 500,000 connected devices were vulnerable to Mirai because of an exploitable component from a single vendor's management software.[5] Manufacturers today are flooding the market with cheap, insecure devices, with few market incentives to design the products with security in mind, or to provide ongoing support. And buyers seem unable to make informed decisions between products based on their competing security features, in part because there are no clear metrics. Because the producers of these insecure IoT devices currently are insulated from any standards requirements, market feedback, or liability concerns, I am deeply concerned that we are witnessing a 'tragedy of the commons' threat to the continued functioning of the internet, as the security so vital to all internet users remains the responsibility of none.[6] Further, buyers have little recourse when, despite their best efforts, security failures occur.

Under the Federal Communications Commission's (FCC's) Open Internet rules, ISPs cannot prohibit the attachment of "non-harmful devices" to their networks. It seems entirely reasonable to conclude under the present circumstances, however, that devices with certain insecure attributes could be deemed harmful to the "network" – whether the ISP's own network or the networks to which it is connected. While remaining vigilant to ensure that such prohibitions do not serve as a pretext for anticompetitive or exclusionary behavior, I would encourage regulators to provide greater clarity to internet service providers in this area.

[4] *See* Liron Segal, *Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps DDoS Attack on OVH*, F5 Features (October 7, 2016), https://f5.com/about-us/news/articles/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-ddos-attack-on-ovh-21937.

[5] *See* Jai Vijayan, *7 Imminent IoT Threats*, Dark Reading (October 21, 2016), http://www.darkreading.com/endpoint/7-imminent-iot-threat-/d/d-id/1327233?image_number=3.

[6] *See* Jeffrey Vagle, *Cybersecurity, Unscrupulous Diners, and Internet Stewardship,* Stanford Center for Internet and Society (October 22, 2016), https://cyberlaw.stanford.edu/blog/2016/10/cybersecurity-unscrupulous-diners-and-internet-stewardship.

DDoS attacks can be powerful tools for censorship, criminal extortion, or nation-state aggression. Tools such as Mirai source code, amplified by an embedded base of insecure devices worldwide, accomplish more than isolated nuisance; these are capabilities – weapons even – that can debilitate entire ranges of economic activity.[7] While the internet was not designed with security in mind, its *resiliency* –which serves as its animating principle – is now being undermined.

I respectfully request that you respond to the following questions:

1. What types of network management practices are available for internet service providers to respond to DDoS threats? In the FCC's Open Internet Order, the Commission suggested that ISPs could take such steps only when addressing "traffic that constitutes a denial-of-service attack on specific network infrastructure elements." Is it your agency's opinion that the Mirai attack has targeted "specific network infrastructure elements" to warrant a response from ISPs?

2. Would it be a reasonable network management practice for ISPs to designate insecure network devices as "insecure" and thereby deny them connections to their networks, including by refraining from assigning devices IP addresses? Would such practices require refactoring of router software, and if so, does this complicate the feasibility of such an approach?

3. What advisories to, or direct engagement with, retailers of IoT devices have you engaged in to alert them of the risks of certain devices they sell? Going forward, what attributes would help inform your determination that a particular device poses a risk warranting notice to retailers or consumers?

4. What strategies would you pursue to take devices deemed harmful to the network out of the stream of commerce? Are there remediation procedures vendors can take, such as patching? What strategy would you pursue to deactivate or recall the embedded base of consumer devices?

5. What consumer advisories have you issued to alert consumers to the risks of particular devices?

6. Numerous reports have indicated that users often fail to install relevant updates, despite their availability.[8] To the extent that certain device security capabilities can be improved with software or firmware updates, how will you ensure that these updates are implemented?

[7] See Bruce Schneier, *Someone Is Learning How To Take Down The Internet*, Schneier on Security (October 6, 2016), https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html.

[8] See Jennifer Valentino-Devries, *Rarely Patched Software Bugs in Home Routers Cripple Security*, Wall Street Journal (January 18, 2016), http://www.wsj.com/articles/rarely-patched-software-bugs-in-home-routers-cripple-security-1453136285.

7. Do consumers have meaningful ability to distinguish between products based on their security features? Are formal, or third-party, metrics needed to establish a baseline for consumers to evaluate products? If so, has your agency taken steps to create or urge the creation of such a baseline?

8. Should manufacturers have to abide by minimum technical security standards? Has your agency discussed the possibility of establishing meaningful security standards with the National Institute of Standards and Technology?

9. What is the feasibility, including in terms of additional costs to manufacturers, of device security testing and certification, akin to current equipment testing and certification of technical standards conducted by the Federal Communications Commission under 47 CFR Part 2?

I look forward to your response. If you should have any questions or concerns, please contact Rafi Martina in my office at 202-224-2023.

Sincerely,

Mark R Warner

Mark R. Warner
United States Senator

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

December 2, 2016

The Honorable Mark Warner
United States Senate
475 Russell Senate Office Building
Washington, D.C. 20510

Dear Senator Warner:

Thank you for your letter regarding the important issue of Distributed Denial of Service (DDoS) attacks, the security of the nation's networks, and the equipment and devices that attach to the networks to deliver integrated Internet-powered services to citizens and businesses.

Cybersecurity has been a top priority for the Commission during my tenure. As you note, the rapid growth of network-connected consumer devices creates particular cybersecurity challenges. The Commission's oversight of our country's privately owned and managed communications networks is an important component of the larger effort to protect critical communications infrastructure and the American public from malicious cyber actors. The Commission is uniquely situated to comprehensively address this issue given its authority over the use of radio spectrum as well as the connections to and interconnections between commercial networks, which touch virtually every aspect of our economy. Other agencies have also begun looking at network-connected devices and the security implications they bring in certain industry segments.[1]

As your letter suggests, the Commission's *Open Internet Order*'s rules enable Internet Service Providers (ISPs) to take measures to protect their networks, and those with which they interconnect, from harmful devices. These rules make clear that providers not only have the latitude to take actions to protect consumers from harm, but have the responsibility to do so. The *Open Internet Order* in particular emphasizes that reasonable network management incorporates practices "ensuring network security and integrity," including by "addressing traffic harmful to the network," such as denial of service attacks.[2] The *Open Internet Order* thus affirms ISPs'

[1] For example, the U.S. Food and Drug Administration released draft guidance outlining the agency's expectations for monitoring, identifying and addressing cybersecurity vulnerabilities in medical devices once they have entered the market. *See* U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (2016), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf. The U.S. Department of Transportation has proposed guidance on improving motor vehicle cybersecurity. *See* U.S. Department of Transportation, Cybersecurity Best Practices for Modern Vehicles (2016), http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[2] *See Protecting and Promoting the Open Internet*, Report and Order, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5701, para. 220 (2015), *aff'd, United States Telecom v. FCC*, 825 F.3d 674 (D.C. Cir. 2016).

ability to take measures to protect the network. This policy builds on FCC rules that have, for decades, given providers of wireline telecommunications the right to "temporarily discontinue service forthwith" in the face of imminent harm.[3] More broadly, the recent D.C. Circuit decision upholding the Commission's authority over broadband networks empowers it to address core network issues.

In recognition of the Commission's authority over telecommunications networks, Commission staff have been actively examining cyber challenges presented by today's end-to-end Internet environment. This environment is fundamentally different, and more challenging, than the legacy telecommunications security environment that we've managed risks under for decades. The Dyn DDoS attack is illustrative of the cyber challenges that the Commission faces. During the attack, insecure devices, connected through wireless networks, shut down service to millions of customers by attacking a domain name system (DNS) server of an entity not licensed or directly regulated by the Commission. This attack highlighted that security vulnerabilities induced by or inherent in devices now can have large-scale impacts on network services connecting those devices. This is particularly so in two areas relevant to the Dyn attack: (i) the services at issue enable a broad new array of security risks to individuals and businesses that providers only have a defined and limited role in managing; and (ii) the many new entities involved in the end-to-end consumer Internet experience (especially with respect to IoT). As the end-to-end Internet user experience continues to expand and diversify, both through provider network inputs and the products and services enabled by Internet access, the Commission's ability to provide assurance to individuals and businesses against cyber risk will continue to be both taxed and constrained.

To protect consumers using telecommunications networks, the Commission must address these cyber challenges. In 2014, I initiated a new paradigm for how the FCC would address cybersecurity for our nation's communications networks and services. I stated that it begins with private sector leadership that recognizes how easily cyber threats cross corporate and national boundaries and that, because of this, the communications sector must step up its responsibility and accountability for cyber risk management. In this vein, the Commission has worked closely with its Federal Advisory Committees, as well as with our federal partners and other stakeholders, to foster standards and best practices for cyber risk management.[4] We worked with the other regulatory agencies to create a forum whereby the agency principles meet to share best cybersecurity regulatory practices and coordinate our approaches. As a result of these collaborative efforts, a rich body of recommendations, including voluntary best practices, have been developed. Industry implementation of these practices must be part of any cybersecurity solution.

[3] *See* 47 CFR 68.108.

[4] For example, our Technological Advisory Council (TAC) has been examining how to incorporate "security by design" principles into the very fabric of emerging 5G networks, and our Communications Security, Reliability, and Interoperability Council (CSRIC) has been working on cybersecurity in connection with a number of issues, such as improving supply chain risk management, addressing risks associated with legacy protocols such as SS7, and promoting security in networks and devices utilizing Wi-Fi technology. In addition, we have been preparing to launch voluntary, face-to-face engagements, consistent with NIST Framework and CSRIC recommendations, in which providers will collaborate with the Commission to address cyber risk issues in their networks and service environments.

I do, however, share your concern that we cannot rely solely on the market incentives of ISPs to fully address the risk of malevolent cyber activities. As private actors, ISPs operate in economic environments that pressure them to not take those steps, or to take them minimally. Given the interconnected nature of broadband networks, protective actions taken by one ISP against cyberthreats can be undermined by the failure of other ISPs to take similar actions. This weakens the incentive of all ISPs to take such protections. Cyber-accountability therefore requires a combination of market-based incentives and appropriate regulatory oversight where the market does not, or cannot, do the job effectively.

While we have had to postpone some of the next steps in this combined approach in light of the impending change in Administrations, addressing IoT threats remains a National imperative and should not be stalled by the normal transition of a new president. In recognition of the critical importance of the work that remains to protect Americans from cyber threats, I've attached an outline of a program that I believe would reduce the risk of cyber threats to America's citizens and businesses. This program includes collaborative efforts with key Internet stakeholder groups; increased interagency cooperation; and consideration of regulatory solutions by the Commission to address residual risk that cannot be addressed by market forces alone due to market failure.

Thank you for your interest in this important issue. Your views are very important and will be included in the record of this proceeding. I would be happy to make appropriate FCC staff available to you and your staff for additional discussions regarding our ongoing work on these important issues. I also stand ready to collaborate on these efforts with my colleagues in a bipartisan manner during the remainder of my term.

Sincerely,

Tom Wheeler

5G/IoT CYBERSECURITY RISK REDUCTION PROGRAM PLAN

1. Federal Advisory Committee/voluntary stakeholder engagement.

- Charge the FCC's Federal Advisory Committees to develop cyber risk reduction standards and best practices and to promote ISP-wide adoption and implementation of those standards. In particular, convene an advisory group with broad-based cyber expertise, including industry, academia, and government agencies to provide recommendations for a device cybersecurity certification process.
- Establish an advisory committee/working group to provide recommendations on what different members of the communications ecosystem (including 5G service providers, 5G network equipment manufacturers and suppliers, and 5G device manufacturers and suppliers) should do to prevent, reduce the risk of, or mitigate edge-based attacks that cause harm to the network.
- Conduct voluntary and confidential, provider-specific meetings in which cyber threat and risk reduction challenges can be candidly discussed in order to foster a collaborative relationship and continued dialogue between the communications sector and the Commission.

2. Leverage interagency relationships.

- Provide the Cybersecurity Forum for Independent and Executive Branch Regulators to coordinate regulatory approaches to address IoT residual risks across the broader regulatory environment.
- Within the Forum, convene a task force composed of cybersecurity regulatory experts in the relevant agencies to assess the full scope of IoT cyber threats to critical infrastructure, existing regulatory authorities and mitigation recommendations within those authorities, as well as those authorities requiring statutory change.
- Continue collaboration with our executive branch partners, state, local, Tribal, and territorial entities to identify unique state and local challenges and champion near-term activity to address those needs.

3. Regulatory/rulemaking activities.

- Identify cybersecurity data gaps with respect to residual risk in our network outage reporting framework and develop reporting obligations to address these gaps, in order to ensure the FCC has situational awareness during and immediately after major communications disruptions, and to enable the Commission to utilize outage data to formulate standards and best practices to promote the overall reliability and resiliency of the nation's communications networks.
- Issue a Notice of Inquiry to develop a record and identify residual risk in the IoT commons, with the goal of determining where market failure may exist in the ISP, network element manufacturer, and device manufacturer community; identify current security best practices that could be implemented now by communications service providers—such as network filtering techniques—to address DoS attacks; and identify

methods third party solution providers and other stakeholders in the 5G ecosystem can take to mitigate DoS attacks.

- Issue an NPRM to examine regulatory measures the FCC could take to help address cyber risks that cannot be addressed through market-based measures.
    - Consider the application of existing legal authorities to protect networks from IoT device security risks. The NPRM could examine changes to the FCC's equipment certification process to protect networks from IoT device security risks. Equipment authorization is a critical element of the FCC's regulatory structure to maintain the integrity and usability of spectrum.
    - Explore the potential of a cybersecurity certification (possibly self-certification) to create a floor and identifiable risk relevant levels above the floor for device cybersecurity and a consumer labeling requirement to address any asymmetry in the availability of information and help consumers understand and make better decisions regarding the potential cyber risks of a product or service.
    - Work with the Broadband Technical Advisory Group (BITAG) and 5G/IoT relevant stakeholder groups to build upon the evolving risk reduction initiatives, encouraging industry-initiated commitment as the preferred option and increased government engagement where that falls short.